

[Discussion Draft]**AMENDMENT TO H. RES. 164****OFFERED BY M** .

At the end of the resolution, add the following:

1 SEC. 2. Notwithstanding any other provision of this
2 resolution, the amendment specified in section 3 shall be
3 in order as though printed as the last amendment in
4 House Report 113–41 if offered by Representative McCaul
5 of Texas or his designee. That amendment shall be debat-
6 able for 10 minutes equally divided and controlled by the
7 proponent and an opponent.

8 SEC. 3. The amendment referred to in section 2 is
9 as follows: After section 1, insert the following new section
10 (and renumber subsequent sections accordingly):

11 **“SEC. 2. FEDERAL GOVERNMENT COORDINATION WITH RE-**
12 **SPECT TO CYBERSECURITY.**

13 “(a) COORDINATED ACTIVITIES.—The Federal Gov-
14 ernment shall conduct cybersecurity activities to provide
15 shared situational awareness that enables integrated oper-
16 ational actions to protect, prevent, mitigate, respond to,
17 and recover from cyber incidents.

18 “(b) COORDINATED INFORMATION SHARING.—

1 “(1) DESIGNATION OF COORDINATING ENTITY
2 FOR CYBER THREAT INFORMATION.—The President
3 shall designate an entity within the Department of
4 Homeland Security as the civilian Federal entity to
5 receive cyber threat information that is shared by a
6 cybersecurity provider or self-protected entity in ac-
7 cordance with section 1104(b) of the National Secu-
8 rity Act of 1947, as added by section 3(a) of this
9 Act, except as provided in paragraph (2) and subject
10 to the procedures established under paragraph (4).

11 “(2) DESIGNATION OF A COORDINATING ENTI-
12 TY FOR CYBERSECURITY CRIMES.—The President
13 shall designate an entity within the Department of
14 Justice as the civilian Federal entity to receive cyber
15 threat information related to cybersecurity crimes
16 that is shared by a cybersecurity provider or self-
17 protected entity in accordance with section 1104(b)
18 of the National Security Act of 1947, as added by
19 section 3(a) of this Act, subject to the procedures
20 under paragraph (4).

21 “(3) SHARING BY COORDINATING ENTITIES.—
22 The entities designated under paragraphs (1) and
23 (2) shall share cyber threat information shared with
24 such entities in accordance with section 1104(b) of
25 the National Security Act of 1947, as added by sec-

1 tion 3(a) of this Act, consistent with the procedures
2 established under paragraphs (4) and (5).

3 “(4) PROCEDURES.—Each department or agen-
4 cy of the Federal Government receiving cyber threat
5 information shared in accordance with section
6 1104(b) of the National Security Act of 1947, as
7 added by section 3(a) of this Act, shall establish pro-
8 cedures to—

9 “(A) ensure that cyber threat information
10 shared with departments or agencies of the
11 Federal Government in accordance with such
12 section 1104(b) is also shared with appropriate
13 departments and agencies of the Federal Gov-
14 ernment with a national security mission in real
15 time;

16 “(B) ensure the distribution to other de-
17 partments and agencies of the Federal Govern-
18 ment of cyber threat information in real time;
19 and

20 “(C) facilitate information sharing, inter-
21 action, and collaboration among and between
22 the Federal Government; State, local, tribal,
23 and territorial governments; and cybersecurity
24 providers and self-protected entities.

25 “(5) PRIVACY AND CIVIL LIBERTIES.—

1 “(A) POLICIES AND PROCEDURES.—The
2 Secretary of Homeland Security, the Attorney
3 General, the Director of National Intelligence,
4 and the Secretary of Defense shall jointly estab-
5 lish and periodically review policies and proce-
6 dures governing the receipt, retention, use, and
7 disclosure of non-publicly available cyber threat
8 information shared with the Federal Govern-
9 ment in accordance with section 1104(b) of the
10 National Security Act of 1947, as added by sec-
11 tion 3(a) of this Act. Such policies and proce-
12 dures shall, consistent with the need to protect
13 systems and networks from cyber threats and
14 mitigate cyber threats in a timely manner—

15 “(i) minimize the impact on privacy
16 and civil liberties;

17 “(ii) reasonably limit the receipt, re-
18 tention, use, and disclosure of cyber threat
19 information associated with specific per-
20 sons that is not necessary to protect sys-
21 tems or networks from cyber threats or
22 mitigate cyber threats in a timely manner;

23 “(iii) include requirements to safe-
24 guard non-publicly available cyber threat
25 information that may be used to identify

1 specific persons from unauthorized access
2 or acquisition;

3 “(iv) protect the confidentiality of
4 cyber threat information associated with
5 specific persons to the greatest extent
6 practicable; and

7 “(v) not delay or impede the flow of
8 cyber threat information necessary to de-
9 fend against or mitigate a cyber threat.

10 “(B) SUBMISSION TO CONGRESS.—The
11 Secretary of Homeland Security, the Attorney
12 General, the Director of National Intelligence,
13 and the Secretary of Defense shall, consistent
14 with the need to protect sources and methods,
15 jointly submit to Congress the policies and pro-
16 cedures required under subparagraph (A) and
17 any updates to such policies and procedures.

18 “(C) IMPLEMENTATION.—The head of
19 each department or agency of the Federal Gov-
20 ernment receiving cyber threat information
21 shared with the Federal Government under
22 such section 1104(b) shall—

23 “(i) implement the policies and proce-
24 dures established under subparagraph (A);
25 and

1 “(ii) promptly notify the Secretary of
2 Homeland Security, the Attorney General,
3 the Director of National Intelligence, the
4 Secretary of Defense, and the appropriate
5 congressional committees of any significant
6 violations of such policies and procedures.

7 “(D) OVERSIGHT.—The Secretary of
8 Homeland Security, the Attorney General, the
9 Director of National Intelligence, and the Sec-
10 retary of Defense shall jointly establish a pro-
11 gram to monitor and oversee compliance with
12 the policies and procedures established under
13 subparagraph (A).

14 “(6) INFORMATION SHARING RELATIONSHIPS.—
15 Nothing in this section shall be construed to—

16 “(A) alter existing agreements or prohibit
17 new agreements with respect to the sharing of
18 cyber threat information between the Depart-
19 ment of Defense and an entity that is part of
20 the defense industrial base;

21 “(B) alter existing information-sharing re-
22 lationships between a cybersecurity provider,
23 protected entity, or self-protected entity and the
24 Federal Government;

1 “(C) prohibit the sharing of cyber threat
2 information directly with a department or agen-
3 cy of the Federal Government for criminal in-
4 vestigative purposes related to crimes described
5 in section 1104(c)(1) of the National Security
6 Act of 1947, as added by section 3(a) of this
7 Act; or

8 “(D) alter existing agreements or prohibit
9 new agreements with respect to the sharing of
10 cyber threat information between the Depart-
11 ment of Treasury and an entity that is part of
12 the financial services sector.

13 “(7) TECHNICAL ASSISTANCE.—

14 “(A) DISCUSSIONS AND ASSISTANCE.—
15 Nothing in this section shall be construed to
16 prohibit any department or agency of the Fed-
17 eral Government from engaging in formal or in-
18 formal technical discussion regarding cyber
19 threat information with a cybersecurity provider
20 or self-protected entity or from providing tech-
21 nical assistance to address vulnerabilities or
22 mitigate threats at the request of such a pro-
23 vider or such an entity.

24 “(B) COORDINATION.—Any department or
25 agency of the Federal Government engaging in

1 an activity referred to in subparagraph (A)
2 shall coordinate such activity with the entity of
3 the Department of Homeland Security des-
4 ignated under paragraph (1) and share all sig-
5 nificant information resulting from such activity
6 with such entity and all other appropriate de-
7 partments and agencies of the Federal Govern-
8 ment.

9 “(C) SHARING BY DESIGNATED ENTITY.—
10 Consistent with the policies and procedures es-
11 tablished under paragraph (5), the entity of the
12 Department of Homeland Security designated
13 under paragraph (1) shall share with all appro-
14 priate departments and agencies of the Federal
15 Government all significant information resulting
16 from—

17 “(i) formal or informal technical dis-
18 cussions between such entity of the De-
19 partment of Homeland Security and a cy-
20 bersecurity provider or self-protected entity
21 about cyber threat information; or

22 “(ii) any technical assistance such en-
23 tity of the Department of Homeland Secu-
24 rity provides to such cybersecurity provider

1 or such self-protected entity to address
2 vulnerabilities or mitigate threats.

3 “(c) REPORTS ON INFORMATION SHARING.—

4 “(1) INSPECTOR GENERAL OF THE DEPART-
5 MENT OF HOMELAND SECURITY REPORT.—The In-
6 spector General of the Department of Homeland Se-
7 curity, in consultation with the Inspector General of
8 the Department of Justice, the Inspector General of
9 the Intelligence Community, the Inspector General
10 of the Department of Defense, and the Privacy and
11 Civil Liberties Oversight Board, shall annually sub-
12 mit to the appropriate congressional committees a
13 report containing a review of the use of information
14 shared with the Federal Government under sub-
15 section (b) of section 1104 of the National Security
16 Act of 1947, as added by section 3(a) of this Act,
17 including—

18 “(A) a review of the use by the Federal
19 Government of such information for a purpose
20 other than a cybersecurity purpose;

21 “(B) a review of the type of information
22 shared with the Federal Government under
23 such subsection;

24 “(C) a review of the actions taken by the
25 Federal Government based on such information;

1 “(D) appropriate metrics to determine the
2 impact of the sharing of such information with
3 the Federal Government on privacy and civil
4 liberties, if any;

5 “(E) a list of the departments or agencies
6 receiving such information;

7 “(F) a review of the sharing of such infor-
8 mation within the Federal Government to iden-
9 tify inappropriate stovepiping of shared infor-
10 mation; and

11 “(G) any recommendations of the Inspec-
12 tor General of the Department of Homeland Se-
13 curity for improvements or modifications to the
14 authorities under such section.

15 “(2) PRIVACY AND CIVIL LIBERTIES OFFICERS
16 REPORT.—The Officer for Civil Rights and Civil
17 Liberties of the Department of Homeland Security,
18 in consultation with the Privacy and Civil Liberties
19 Oversight Board, the Inspector General of the Intel-
20 ligence Community, and the senior privacy and civil
21 liberties officer of each department or agency of the
22 Federal Government that receives cyber threat infor-
23 mation shared with the Federal Government under
24 such subsection (b), shall annually and jointly sub-
25 mit to Congress a report assessing the privacy and

1 civil liberties impact of the activities conducted by
2 the Federal Government under such section 1104.
3 Such report shall include any recommendations the
4 Civil Liberties Protection Officer and Chief Privacy
5 and Civil Liberties Officer consider appropriate to
6 minimize or mitigate the privacy and civil liberties
7 impact of the sharing of cyber threat information
8 under such section 1104.

9 “(3) FORM.—Each report required under para-
10 graph (1) or (2) shall be submitted in unclassified
11 form, but may include a classified annex.

12 “(d) DEFINITIONS.—In this section:

13 “(1) APPROPRIATE CONGRESSIONAL COMMIT-
14 TEES.—The term ‘appropriate congressional com-
15 mittees’ means—

16 “(A) the Committee on Homeland Secu-
17 rity, the Committee on the Judiciary, the Per-
18 manent Select Committee on Intelligence, and
19 the Committee on Armed Services of the House
20 of Representatives; and

21 “(B) the Committee on Homeland Security
22 and Governmental Affairs, the Committee on
23 the Judiciary, the Select Committee on Intel-
24 ligence, and the Committee on Armed Services
25 of the Senate.

1 “(2) CYBER THREAT INFORMATION, CYBER
2 THREAT INTELLIGENCE, CYBERSECURITY CRIMES,
3 CYBERSECURITY PROVIDER, CYBERSECURITY PUR-
4 POSE, AND SELF-PROTECTED ENTITY.—The terms
5 ‘cyber threat information’, ‘cyber threat intelligence’,
6 ‘cybersecurity crimes’, ‘cybersecurity provider’, ‘cy-
7 bersecurity purpose’, and ‘self-protected entity’ have
8 the meaning given those terms in section 1104 of
9 the National Security Act of 1947, as added by sec-
10 tion 3(a) of this Act.

11 “(3) INTELLIGENCE COMMUNITY.—The term
12 ‘intelligence community’ has the meaning given the
13 term in section 3(4) of the National Security Act of
14 1947 (50 U.S.C. 401a(4)).

15 “(4) SHARED SITUATIONAL AWARENESS.—The
16 term ‘shared situational awareness’ means an envi-
17 ronment where cyber threat information is shared in
18 real time between all designated Federal cyber oper-
19 ations centers to provide actionable information
20 about all known cyber threats.”.

21 Page 5, strike line 6 and all that follows through page
22 6, line 7.

23 Page 7, beginning on line 17, strike “by the department
24 or agency of the Federal Government receiving such cyber
25 threat information”.

- 1 Page 13, strike line 13 and all that follows through page
- 2 15, line 23. Page 17, strike line 15 and all that follows
- 3 through page 19, line 19.
- 4 Page 17, strike line 15 and all that follows through page
- 5 19, line 19.

